REMARKS

In the Office Action dated May 2, 2007, claims 1-5, 7-15, 17-24 and 26-28 were rejected under 35 USC § 102(e) as anticipated by Cheline et al. US Patent Publication No. 2003/0041136 ("Cheline").

Claims 6, 16 and 25 were rejected under 35 USC § 103 as being unpatentable over Cheline in view of Nguyen et al. US Patent Publication No. 2003/0172145 ("Nguyen").

Applicants submit that Cheline, alone or in combination with Nguyen, does not disclose, teach or suggest what is recited in any of the pending claims. Applicants' invention is directed principally at making a network less susceptible to malicious code introduced inadvertently by authorized users who connect to the network over a VPN connection. To achieve this end, Applicants' have devised methods and systems that carefully regulate network access of and write access to a VPN capable end system. Cheline addresses a more conventional remote access VPN that shows no particular concern for Applicants' inventive goals and is not suited to achieve them. Nguyen for its part merely mentions, with little elaboration, that ISPs may deploy VPN technology to enhance security. The differences between Cheline and Nguyen, on the one hand, and Applicants' invention, on the other, are stark and manifest themselves in numerous elements recited or incorporated in each and every pending claim.

Cheline Does Not Anticipate Claims 1-5, 7-15, 17-24 and 26-28

Regarding claims 1-5, 7-15, 17-24 and 26-28, Cheline first fails to teach or disclose denying network access to a VPN capable end system before a user on the end system becomes authenticated. In Cheline, the client computer 102 is an end system. However, the VPN client software that has security procedures 226 (i.e. the RADIUS client) resides on the modem 106 which is not part of the client computer 102. This is

done purposely "to alleviate[] drawbacks associated with software interoperability and maintenance issues on the user's client computer." ¶ [0028] and FIG. 2. Meanwhile, the client computer 102 is connected to other client computers on a local area network that does not traverse the modem 106, and there is no indication to deny the client computer 102 access to this local area network before a user of the client computer 102 becomes authenticated. ¶ [0031] and FIG. 1.

Further regarding claims 1-5, 7-15, 17-24 and 26-28, Cheline fails to teach or disclose permitting network access by the end system solely on at least one VPN connection to an enterprise network once the user on the end system becomes authenticated. The Examiner appears to have neglected the term "solely" in this claim limitation. While Cheline discloses to provide VPN access to authenticated users of the client computer 102, there is no indication that this VPN access is the sole or exclusive form of network access permitted to the client computer 102. Indeed, as already mentioned, the client computer 102 is connected to other client computers on a local area network behind the modem 106 that hosts the VPN client software, and there is no indication that access to that local area network is denied to the client computer 102 before or after the user on the client computer 102 authenticates.

Further regarding claims 1-5, 7-15, 17-24 and 26-28, Cheline fails to teach or disclose permitting write access to the end system solely to at least one temporary memory while the VPN connection is active. For alleged correspondence to this claim limitation, the Examiner cites to ¶ [0049] of Cheline which merely indicates that information is transferred on the established VPN between the client computer 102 and the server-side system. However, permitting write access solely to a temporary memory of the client computer 102 cannot be inferred from mere information transfer between the client computer 102 and the server-side system. Such information transfer might instead involve no write access to the client computer 102 at all, or write access solely to a permanent memory of the client computer 102, or write access

to both a permanent memory and a temporary memory of the client computer 102, for example.

Regarding claim 2, Cheline also fails to teach or disclose performing the denying and permitting steps of claim 1 on an end system. As mentioned, in Cheline the VPN client software resides on the modem 106 rather than on the client computer 102. ¶ [0028]. Thus, even if the VPN client software in Cheline were indicated to perform the permitting and denying steps recited in claim 1 (which it doesn't), these steps would still not be performed on an end system. The Examiner cites to ¶ ¶ [0043], [0049], [0069] and [0071] for alleged correspondence with claim 2; however, these paragraphs discuss executing VPN security procedures 226 on the modem 106--which is not an end system.

Regarding claims 3, 14 and 23, Cheline also fails to teach or disclose purging the temporary memory once the VPN connection becomes inactive. Here, the Examiner cites to ¶ [0076] of Cheline which indicates that the VPN tunnel is torn-down if no VPN traffic is detected for a predetermined length of time. However, there is no indication that tear-down of the VPN tunnel in Cheline results in purging of any memory, much less purging a temporary memory on an end system that was the only memory on the end system to which write access had been permitted while the VPN connection was active. Indeed, the only temporary memory mentioned in Cheline is cache 236. ¶ [0058] and FIG. 2. Cache 236 resides on the modem 106, which is not an end system, and there is no indication that cache 236 is purged once the VPN connection becomes inactive.

Regarding claims 7 and 21, Cheline also fails to teach or disclose directing data writes to a RAM disk on the end system. The Examiner cites to ¶ [0071] of Cheline which indicates that a VPN connection is established between the client computer 102 and the server-side system. However, directing data writes to a RAM disk of the client

computer 102 cannot be inferred from VPN establishment. Indeed, Cheline makes no mention of a RAM disk on the client computer 102.

Regarding claims 9, 10, 18, 19, 27 and 28, Cheline also fails to teach or disclose restarting or shutting down the end system once the VPN connection becomes inactive. The Examiner cites to ¶ [0071] of Cheline which indicates that the VPN connection is dropped if traffic is not transmitted on the VPN for a predetermined length of time. However, there is no indication in Cheline that dropping the VPN connection triggers a restart or shut-down of the client computer 102.

Regarding claims 13-15, 17-24 and 26-28, Cheline also fails to teach or disclose operating system software on or for a VPN capable end system for denying network access to the end system before a user on the end system becomes authenticated, permitting network access by the end system solely on at least one VPN connection to an enterprise network once the user on the end system becomes authenticated and permitting write access to the end system solely to at least one temporary memory while the VPN connection is active. As discussed, in Cheline the VPN client software which has security procedures 226 resides on the modem 106 rather than on the client computer 102. ¶ [0028]. Thus, even if there were an indication in Cheline to deny and permit as recited in claims 13 and 22 (which there isn't), these permissions and denials would not be performed by operating software on an end system.

The Combination of Cheline and Nguyen Does Not Render Claims 6, 16 and 25 Unpatentable for Obviousness

Claims 6, 16 and 25 depend from claims 1, 13 and 22, respectively, which are allowable for reasons set forth above. Claims 6, 16, and 25 are therefore also allowable for the reasons set forth above.

Furthermore, Nguyen fails to teach or disclose dropping packets that are not associated with the VPN connection. The Examiner cites to ¶ [1087] of Nguyen which indicates that a firewall may drop attempted connections that are not associated with an authorized protocol, source address or destination address. This discussion of firewalls appears unrelated to the mention of VPN technology almost one hundred paragraphs earlier in that published application. Moreover, with regard to claims 16 and 25, there is no discussion in Nguyen to have operating software on the end system perform a dropping function to prevent communication outside the VPN.

In view of the foregoing, consideration and favorable action on all claims are respectfully requested. Accordingly, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Should any question remain in view of this communication, the Examiner is encouraged to call the undersigned so that a prompt disposition of this application can be achieved.

Respectfully submitted,

Scot A. Reader
Registration Number 39,002
Telephone No. (303) 440-4050
Scot A. Reader, P.C.
1320 Pearl Street
Suite 228
Boulder, CO 80302